

**REMARKS**

This application has been carefully reviewed in view of the above-referenced Office Action, and reconsideration is requested in view of the following remarks.

**Regarding the Rejection under 35 U.S.C. §112**

Claim 12 has been amended to correct the antecedent basis error noted by the Examiner.

**Regarding the Rejections under 35 U.S.C. §102**

All claims were rejected as anticipated by the So reference of record. The So reference relates to a video-on-demand (VOD) system that uses conditional access methods in conjunction with ECM retrofitting to control access to pre-encrypted VOD content.

**Regarding Claim 1**

It is noted that claim 1 calls for "*determining if the request is from a terminal having decryption capabilities associated with a first decryption method or a second decryption method*". The Office Action asserts that this claim feature is met by paragraph 63, where the CAS system determines cryptographic parameters. In fact, paragraph 63 states that "*CAS 110 permits access to the pre-encrypted content by subscriber terminals with EMMs, and generating ECMs for non-VOD services. Other functions of the CAS include ... transmitting cable system-specific cryptographic parameters (e.g., periodical keys) to the encryption renewal system to enable ECM retrofitting.*" Hence, the relevant disclosure of paragraph 63 only discloses that the conditional access system provides subscriber terminals with EMM or ECM messages and sends system specific information to an ECM retrofitting process. Nothing in this paragraph, or in So in general, appears to meet the claim requirements of determining if a terminal has decryption capabilities associated with a first or second decryption method.

It is further noted that as of this point in the claim, first and second portions of the content have been selected and stored, but the claim does not as of this point call for actual encryption. This is in contrast with So which calls for pre-encryption using an off-line encryption system (OLES) (see, for example, paragraphs [0017], [0034], [0042], [0046] and [0047]).

Application No.: 10/823,431

Claim 1 further calls for "*if the request is from a terminal having decryption capabilities associated with the first decryption method, then: routing the first portions to a first encryption device; routing the second portions around the first encryption device; encrypting the first portions using a first encryption process at the first encryption device to produce encrypted first portions; and assembling a stream of selectively encrypted content from the encrypted first portions and the second portions.*" (*emphasis added*) It is particularly noted that the process just described is contradictory to the teachings of So, which uses an OLES to pre-encrypt and store the content (again see, for example, paragraphs [0017], [0034], [0042], [0046] and [0047]). In contrast, to paraphrase without intent of imposing limitations, claim 1 calls for first portions to be routed to a first encryption device, second portions to bypass the first encryption device, and a selectively encrypted stream to be assembled therefrom. It is further noted that this selective encryption process is predicated on the request coming from a terminal having first decryption capabilities as a result of the determination made as discussed previously. So contains no teaching or suggestion of this, and in fact, teaches against it. Hence, there can be no anticipation of claim 1. Additionally, no mechanism is shown in So for bypassing encryption and assembly of a selectively encrypted stream as claimed. In fact, So specifically notes that his OLES system used for pre-encryption is not shown (see paragraph [0053]). Hence, even if So were to carry out these functions, his disclosure is non-enabling as to these functions.

In addition, the Office Action submits that selective encryption is taught at paragraph [0106]. However, it is noted that paragraph [0106] provides a quite narrow interpretation of the term "selective encryption" in the sense that encryption is used on packets having a scrambling control field that is set to 1x. This is in contrast to paragraph [0108] which describes encryption without regard for the scrambling control field. There is no teaching or suggestion of the selective encryption as claimed in response to a determination as to encryption capabilities of a recipient terminal device.

So additionally fails to disclose or suggest selection of the first and second portions of content and then storing them as claimed. Instead, So pre-encrypts the content and then stores it along with an associated encryption record.

In light of all of the above, it is clear that claim 1 is not anticipated by So.

Application No.: 10/823,431

Regarding Claims 2-10

Claims 2-10 are dependent from claim 1. Although additional distinctions exist, in view of the above clear failure of So to meet each feature of claim 1, these claims need not be further addressed at this time, since they exhibit at least the same distinctions over So. Hence, there can be no anticipation of claims 2-10.

Regarding Claims 7 and 11

Each of the above remarks are equally applicable to claims 7 and 11. In addition, claims 7 and 11 call for "*if the request is from a terminal having decryption capabilities associated with the second decryption method, then: assembling a stream of content from the first portion and the second portion; routing the stream to a second encryption device; and encrypting the first portions using a second encryption process at the second encryption device to produce a selectively encrypted stream.*" (*emphasis added*) Again, it is noted that So fails to teach or suggest making a determination of the decryption capabilities of a terminal. Furthermore, if the terminal has second decryption capabilities, an alternative action is carried out wherein the first and second portions are assembled into a stream and the stream is passed to a second encryption device that produces a selectively encrypted stream. It is noted that So only teaches off-line encryption, whereas, the present claims encrypt only after making a determination of decryption capabilities of a recipient terminal upon receipt of a request for content. The encryption process used depends upon the capabilities of the recipient terminal. Moreover, So only teaches a single OLES, presumably capable of encryption using a single encryption algorithm. In contrast, multiple encryption devices that operate using multiple encryption processes are called out in the present claims. In view of these clear distinctions, it is apparent that there can be no anticipation of claims 7 and 11 by So.

Regarding Claims 12-17

Application No.: 10/823,431

Claims 12-17 are dependent from claim 11. Although additional distinctions exist, in view of the above clear failure of So to meet each feature of claim 17, these claims need not be further addressed at this time, since they exhibit at least the same distinctions over So. Hence, there can be no anticipation of claims 12-17.

Regarding Claim 18

Claim 18 is an apparatus claim having features similar to those discussed above in connection with claim 1. Hence, the arguments relating to claim 1 are equally applicable, and there can be no anticipation by So.

Regarding Claim 19

Claim 19 has features similar to those discussed in connection with claims 7 and 11. Hence, the arguments presented above relating to those claims are equally applicable, and there can be no anticipation by So.

Regarding Claims 20-23

Claims 20-23 are dependent from claim 18. Although additional distinctions exist, in view of the above clear failure of So to meet each feature of claim 18, these claims need not be further addressed at this time, since they exhibit at least the same distinctions over So. Hence, there can be no anticipation of claims 20-23.

Regarding Claim 24

Claim 24 is a method claim sharing some features similar to those discussed above in connection with claim 1. Hence, the arguments relating to claim 1 are equally applicable, and there can be no anticipation by So.

Regarding Claims 25-33

Claims 25-33 are dependent from claim 24. Although additional distinctions exist, in view of the above clear failure of So to meet each feature of claim 24, these claims need not be

Application No.: 10/823,431

further addressed at this time, since they exhibit at least the same distinctions over So. Hence, there can be no anticipation of claims 25-33.

Regarding Claim 30

Claim 30 has features similar to those discussed in connection with claims 7 and 11. Hence, the arguments presented above relating to those claims are equally applicable, and there can be no anticipation by So.

Concluding Remarks

Per MPEP 2131, to anticipate Applicants' claims the So reference must teach each and every element of the claims in the arrangement called out in the claims. In view of the above, there is clear failure to establish anticipation. Moreover, the So reference clearly teaches away from techniques that do not use an off-line pre-encryption technique (see, for example, paragraphs [0015] and [0016]). In view of this, not only are the claims not anticipated, they are clearly not rendered *prima facie* obvious by So. Accordingly, reconsideration and allowance are respectfully requested at an early date.

The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, further discussion of each distinction is clearly unnecessary at this time. Failure to address each point raised in the Office Action should accordingly not be viewed as accession to the Examiner's position or an admission of any sort. No amendment made herein was related to the statutory requirements of patentability, but rather to correct a minor error resulting in improper antecedent basis.

In view of this communication, all claims are now believed to be in condition for allowance and such is respectfully requested at an early date. If further matters remain to be resolved, the undersigned respectfully requests the courtesy of a telephone or personal interview. The undersigned can be reached at the telephone number below.

Application No.: 10/823,431

Respectfully submitted,

  
Jerry A. Miller  
Registration No. 30,779  
Dated: 5/24/2006

Please Send Correspondence to:  
Miller Patent Services  
2500 Dockery Lane  
Raleigh, NC 27606  
Phone: (919) 816-9981  
Fax: (919) 816-9982  
**Customer Number 24337**

Application No.: 10/823,431

-14-